

03-03-00

A

THE ASSISTANT COMMISSIONER OF PATENTS  
Washington, D.C. 20231

DOCKET NUMBER: **RP9-99-105**  
March 1, 2000

Sir:

Transmitted herewith for filing is the Patent Application of:

Inventor: **Richard W. Cheston, et al.**

For: **DATA PROCESSING SYSTEM AND METHOD FOR REMOTE RECOVERY OF A PRIMARY PASSWORD**

Enclosed are:

☒ Patent Specification and Executed Declaration

☒ Eight sheets of drawing(s).

☒ An assignment of the invention to International Business Machines Corporation (includes Recordation Form Cover Sheet).

☐ A certified copy of a ☐ application.

☐ Information Disclosure Statement, PTO 1449 and copies of references.

The filing fee has been calculated as shown below:

For	Number Filed	Number Extra	Rate	Fee
Basic Fee				\$690.00
Total Claims	23 - 20	3	x \$18 =	\$ 54.00
Indep. Claims	3 - 3		x \$78 =	\$
MULTIPLE DEPENDENT CLAIM PRESENTED			x \$260 =	\$
TOTAL				\$744.00

☒ Please charge my IBM Corporation Deposit Account No. 50-0563 in the amount of \$744.00. A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to IBM Corporation Deposit Account 50-0563. A duplicate copy of this sheet is enclosed.

☒ Any additional filing fees required under 37 CFR §1.16.

☒ Any patent application processing fees under 37 CFR §1.17.

CERTIFICATE OF MAILING BY "EXPRESS MAIL" UNDER 37 CFR § 1.10

"Express Mail" mailing label number **EL453460937US**

Date of Mailing **March 1, 2000**

I hereby certify that the documents indicated below are being deposited with the United States Postal Service under 37 CFR 1.10 on the date indicated above and are addressed to Box Patent Applications, Assistant Commissioner of Patents, Washington, D.C. 20231 and mailed on the above Date of Mailing with the above "Express Mail" mailing label number

Chris Montez  
(name of person mailing paper)

*Chris Montez*  
SIGNATURE of person mailing paper or fee

Respectfully submitted,

By *Brian F. Russell*  
Brian F. Russell  
Registration No. 40,796  
FELSMAN, BRADLEY, VADEN, GUNTER  
& DILLON, LLP  
Suite 350, Lakewood on the Park  
7600B North Capital of Texas Highway  
Austin, Texas 78731  
Telephone (512) 343-6116

03/01/00  
jc672 U.S. PTO

jc672 U.S. PTO  
09/516430  
03/01/00

09516430-030100

DATA PROCESSING SYSTEM AND METHOD FOR REMOTE  
RECOVERY OF A PRIMARY PASSWORD

**Background of the Invention**

5

**1. Technical Field:**

10

The present invention relates in general to data processing systems and, in particular, to a data processing system and method providing for remotely recovering a primary password required to complete a boot process of a client computer system. Still more particularly, the present invention relates to a data processing system and method for remotely recovering a primary password required to complete a boot process of a client computer system in response to a successful execution of an interrogative password method.

15

**2. Description of the Related Art:**

20

25

30

Personal computer systems are well known in the art. They have attained widespread use for providing computer power to many segments of today's modern society. Personal computers (PCs) may be defined as a desktop, floor standing, or portable microcomputer that includes a system unit having a central processing unit (CPU) and associated volatile and non-volatile memory, including random access memory (RAM) and basic input/output system read only memory (BIOS ROM), a system monitor, a keyboard, one or more flexible diskette drives, a CD-ROM drive, a fixed disk storage drive (also known as a "hard drive"), a pointing device such as a mouse, and an optional network interface adapter. One of the distinguishing characteristics of these systems is the use of a motherboard or system planar to electrically connect

these components together. Examples of such personal computer systems are IBM's PC 300 series, Aptiva series, and Intellistation series.

5           A computer system requires a basic input/output system (BIOS) in order to operate. The BIOS is code that controls basic hardware operations, such as interactions with disk drives, hard drives, and the keyboard.

10           When a computer is reset, a boot process begins when POST begins executing. POST uses the initialization settings to configure the computer. BIOS then controls the basic operation of the hardware utilizing the hardware as it was configured by POST. The boot process is complete upon the completion of the execution of the POST commands.

15           In known systems, after the system has completed its boot process, a password is sometimes used to restrict the use of the system. After the system has been initialized, a user is prompted to enter the correct password. If the correct password is entered, the system will permit access by the user and boot the operating system. If an incorrect password is entered, the system will prohibit access.

20           One of the largest cost problems today for a large corporate information technology (IT) organization is passwords lost by users. When a user has forgotten their password, the user must call the IT help desk and get a new password. Alternatively, a service technician from the IT department may have to physically go to the user's computer system and reset the system so that the user may enter a new password.

25           Therefore a need exists for a data processing system and method for recovering a client computer system's

30

35

primary password from a server computer system prior to the client computer system completing a boot process.

2025 RELEASE UNDER E.O. 14176

## SUMMARY OF THE INVENTION

5 A data processing system and method are disclosed for  
remotely recovering a client computer system's primary  
password. The primary password must be correctly entered  
prior to the client computer system becoming fully  
accessible to a user. The client computer system is coupled  
10 to a server computer system utilizing a network. Prior to  
the client computer system completing a boot process, a user  
is prompted to enter the primary password. An interrogative  
password method is provided in response to an incorrect  
entry of the primary password. The primary password is  
recoverable in response to a successful execution of the  
interrogative password method. The primary password is  
15 recoverable from the server computer system by the client  
computer system prior to the client computer system  
completing the boot process utilizing the interrogative  
password method.

20 The above as well as additional objectives, features,  
and advantages of the present invention will become apparent  
in the following detailed written description.

### BRIEF DESCRIPTION OF THE DRAWINGS

The novel features are set forth in the appended claims. The present invention itself, however, as well as a preferred mode of use, further objectives, and advantages thereof, will best be understood by reference to the following detailed description of a preferred embodiment when read in conjunction with the accompanying drawings, wherein:

**Figure 1** illustrates a pictorial representation of a data processing system including a plurality of client computer systems coupled to a server computer system utilizing a network and a hub in accordance with the method and system of the present invention;

**Figure 2A** depicts a more detailed pictorial representation of a client computer system in accordance with the method and system of the present invention;

**Figure 2B** illustrates a pictorial representation of a special purpose processing unit which is included within a network adapter included within a client computer system in accordance with the method and system of the present invention;

**Figure 3** illustrates a high level flow chart which depicts establishing a unique identifier for each client, and establishing encryption keys for the server and client computer systems in accordance with the method and system of the present invention;

**Figure 4** depicts a high level flow chart which illustrates a client computer system receiving a primary password and a question and answer combination for an interrogative password method in accordance with the method and system of the present invention;

**Figure 5** illustrates a high level flow chart which depicts a server computer system storing a primary password and a question and answer combination for an interrogative password method associated with a particular client computer system in accordance with the method and system of the present invention;

**Figure 6** depicts a high level flow chart which illustrates a server computer system remotely providing a primary password in response to an interrogative password method for a particular client in accordance with the method and system of the present invention; and

**Figure 7** illustrates a high level flow chart which depicts a client computer system permitting a user to access the client in response to a receipt of a primary password from a server computer system in response to a successful execution of an interrogative password method in accordance with the method and system of the present invention.

### DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

A preferred embodiment of the present invention and its advantages are better understood by referring to Figures 1-7 of the drawings, like numerals being used for like and corresponding parts of the accompanying drawings.

The present invention is a method and system for remotely recovering a client computer system's primary password. The client computer system is coupled to a server computer system utilizing a network.

A primary password is established for a client computer system by a user. The primary password must be correctly entered during a boot process of the client in order for the client to complete its boot. If the primary password is not correctly entered, the client will be unable to complete booting, and access to the client will be prohibited.

An alternative password method is described and may be invoked upon an inability to correctly enter the primary password. The alternative password method is an interrogative method which is executed during the client's boot process, and prior to the completion of the boot process. The interrogative method is utilized by a user when the user has been unable to supply the correct primary password. If the interrogative method is executed correctly, the primary password will be supplied remotely by the server.

The interrogative password method includes prompting a user for the answer to a challenge question. If the challenge question is answered correctly, the interrogative method is executed correctly, and the server will supply the



primary password. The client will then complete its boot process.

5 The question and expected answer the client utilizes during the interrogative method are originally supplied by a user. The question and answer are then transmitted by the client to the server along with a client identifier which identifies the particular client supplying the question and answer. The server then stores the question and answer  
10 along with the client identifier to associate the question and answer with this client.

When a client is executing a boot process, if the primary password is not entered correctly, the client will transmit a request to the server for the client's question and answer pair. The server then transmits the question to the client, which then prompts the user for the answer by displaying the question. Once an answer is entered, the client then transmits the answer to the server. The server  
15 will compare the received answer with the expected answer. If they are the same, the server will transmit the client's primary password to the client. The client will then be able to complete its boot process.  
20

25 Transmissions between the client and server are encrypted utilizing an encryption device which includes secure storage. Utilizing the encryption device, the client will encrypt its transmissions with the client's private key and the server's public key. The server will then decrypt  
30 the transmissions received from the client with the client's public key and the server's private key. Likewise, the server will encrypt its transmissions to the client with the server's private key and the client's public key. The client will then decrypt the transmissions received from the

server with the server's public key and the client's private key.

**Figure 1** illustrates a pictorial representation of a network including a plurality of client computer systems **104** coupled to a server computer system **100** utilizing a hub **102** in accordance with the method and system of the present invention. Server computer system **100** is connected to a hub **102** utilizing a local area network (LAN) connector bus **106**. Respective client computer systems **104** also connect to hub **102** through respective LAN busses **106**. The preferred form of the network conforms to the Ethernet specification and uses such hubs and busses. It will be appreciated, however, that other forms of networks may be utilized to implement the invention.

**Figure 2A** depicts a more detailed pictorial representation of a client computer system in accordance with the method and system of the present invention. Client computer system **104** includes a planar (also commonly called a motherboard or system board) which is mounted within client **104** and provides a means for mounting and electrically interconnecting various components of client **104** including a central processing unit (CPU) **200**, system memory **206**, and accessory cards or boards as is well known in the art.

CPU **200** is connected by address, control, and data busses **202** to a memory controller and peripheral component interconnect (PCI) bus bridge **204** which is coupled to system memory **206**. An integrated drive electronics (IDE) device

controller **220**, and a PCI bus to Industry Standard Architecture (ISA) bus bridge **212** are connected to PCI bus bridge **204** utilizing PCI bus **208**. IDE controller **220** provides for the attachment of IDE compatible storage devices, such a removable hard disk drive **222**. PCI/ISA bridge **212** provides an interface between PCI bus **208** and an optional feature or expansion bus such as the ISA bus **214**. PCI/ISA bridge **212** includes power management logic. PCI/ISA bridge **212** is supplied power from battery **244** to prevent loss of configuration data stored in CMOS **213**.

A PCI standard expansion bus with connector slots **210** is coupled to PCI bridge **204**. PCI connector slots **210** may receive PCI bus compatible peripheral cards. An ISA standard expansion bus with connector slots **216** is connected to PCI/ISA bridge **212**. ISA connector slots **216** may receive ISA compatible adapter cards (not shown). It will be appreciated that other expansion bus types may be used to permit expansion of the system with added devices. It should also be appreciated that two expansion busses are not required to implement the present invention.

An I/O controller **218** is coupled to PCI-ISA bridge controller **212**. I/O controller **218** controls communication between PCI-ISA bridge controller **212** and devices and peripherals such as floppy drive **224**, keyboard **226**, and mouse **228** so that these devices may communicate with CPU **200**.

PCI-ISA bridge controller **212** includes an interface for a flash memory **242** which includes an interface for address,

data, flash chip select, and read/write. Flash memory 242 is an electrically erasable programmable read only memory (EEPROM) module and includes BIOS that is used to interface between the I/O devices and operating system.

5

Client computer system 104 includes a video controller 246 which may, for example, be plugged into one of PCI expansion slots 210. Video controller 246 is connected to video memory 248. The image in video memory 248 is read by controller 246 and displayed on a monitor (not shown) which is connected to computer system 104 through connector 250.

10

Computer system 104 includes a power supply 240 which supplies full normal system power 243, and has an auxiliary power main AUX 5 241 which supplies full time power to the power management logic 212.

15

In accordance with the present invention, the planar includes an encryption device 261 which includes an encryption/decryption engine 260 which includes an encryption/decryption algorithm which is utilized to encode and decode messages transmitted and received by the planar, and protected storage 262. Engine 260 can preferably perform public/private key encryption. Engine 260 may access a protected storage device 262. Protected storage device 262 is accessible only through engine 260. Storage device 262 cannot be read or written to by the CPU, device 222, or any other device in the system. The client's unique identifier and its encryption key pair are stored within storage 262. Everything stored in storage 262 is protected by engine 260 and is not directly accessible to the planar

20

25

30

or its components. Device 262 may be implemented utilizing an electronically erasable storage device, such as an EEPROM. Access may be gained to non-readable storage device 262 in order to initially store the client private key.

5 However, after the client private key is stored, it cannot be read. The keys stored in EEPROM 262 may not be read by any component of the planar other than engine 260.

10 Encryption algorithms are known to ensure that only the intended recipient of a message can read and access the message. One known encryption algorithm is an asymmetric, or public key, algorithm. The public key algorithm is a method for encrypting messages sent from a first computer system to a second computer system. This algorithm provides  
15 for a key pair including a public key and a private key for each participant in a secure communication. This key pair is unique to each participant. Examples of such an encryption scheme are an RSA key pair system, and a secure sockets layer (SSL) system.

20 In accordance with the present invention, encryption device 261, including engine 260 and EEPROM 262, is coupled to PCI-ISA bridge 212 utilizing a system management (SM) bus 238. System management bus 238 is a two-wire, low speed,  
25 serial bus used to interconnect management and monitoring devices. Those skilled in the art will recognize that encryption device 261 may be coupled to another bus within the planar.

30 Client 104 also includes a network adapter 230. Network adapter 230 includes a physical layer 234 and a media access controller (MAC) 232 coupled together utilizing

a Media Independent Interface (MII) bus **252**. The MII bus **252** is a specification of signals and protocols which define the interfacing of a 10/100 Mbps Ethernet Media Access Controller (MAC) **232** to the underlying physical layer **234**.

5 Network adapter **230** may be plugged into one of the PCI connector slots **210** (as illustrated) or one of the ISA connector slots **216** in order to permit client **104** to communicate with server **100** utilizing a communication link **106**.

10  
20  
25  
30  
35  
40  
45  
50  
55  
60  
65  
70  
75  
80  
85  
90  
95  
100  
105  
110  
115  
120  
125  
130  
135  
140  
145  
150  
155  
160  
165  
170  
175  
180  
185  
190  
195  
200  
205  
210  
215  
220  
225  
230  
235  
240  
245  
250  
255  
260  
265  
270  
275  
280  
285  
290  
295  
300  
305  
310  
315  
320  
325  
330  
335  
340  
345  
350  
355  
360  
365  
370  
375  
380  
385  
390  
395  
400  
405  
410  
415  
420  
425  
430  
435  
440  
445  
450  
455  
460  
465  
470  
475  
480  
485  
490  
495  
500  
505  
510  
515  
520  
525  
530  
535  
540  
545  
550  
555  
560  
565  
570  
575  
580  
585  
590  
595  
600  
605  
610  
615  
620  
625  
630  
635  
640  
645  
650  
655  
660  
665  
670  
675  
680  
685  
690  
695  
700  
705  
710  
715  
720  
725  
730  
735  
740  
745  
750  
755  
760  
765  
770  
775  
780  
785  
790  
795  
800  
805  
810  
815  
820  
825  
830  
835  
840  
845  
850  
855  
860  
865  
870  
875  
880  
885  
890  
895  
900  
905  
910  
915  
920  
925  
930  
935  
940  
945  
950  
955  
960  
965  
970  
975  
980  
985  
990  
995

MAC **232** processes digital network signals, and serves as an interface between a shared data path, i.e. the MII bus **252**, and the PCI bus **208**. MAC **232** performs a number of functions in the transmission and reception of data packets. For example, during the transmission of data, MAC **232** assembles the data to be transmitted into a packet with address and error detection fields. Conversely, during the reception of a packet, MAC **232** disassembles the packet and performs address checking and error detection. In addition, MAC **232** typically performs encoding/decoding of digital signals transmitted over the shared path and performs preamble generation/removal, as well as bit transmission/reception. In a preferred embodiment, MAC **232** is an Intel 82557 chip. However, those skilled in the art will recognize that the functional blocks depicted in network adapter **230** may be manufactured utilizing a single piece of silicon.

Physical layer **234** conditions analog signals to go out to the network via an R45 connector **236**. Physical layer **234** may be a fully integrated device supporting 10 and 100 Mbps

CSMA/CD Ethernet applications. Physical layer **234** receives parallel data from the MII local bus **252** and converts it to serial data for transmission through connector **236**.

Physical layer **234** is also responsible for wave shaping and provides analog voltages. In a preferred embodiment, physical layer **234** is implemented utilizing an Integrated Services chip ICS-1890.

Physical layer **234** includes auto-negotiation logic that serves three primary purposes. First, it determines the capabilities of client **104**. Second, it advertises its own capabilities to server **100**. And, third, it establishes a connection with server **100** using the highest performance connection technology.

**Figure 2B** illustrates a pictorial representation of special purpose processing unit **300** which is included within a network adapter **230** included within a client computer system **104** in accordance with the method and system of the present invention. Special purpose processing unit is preferably implemented utilizing an ASIC **300** which includes a micro-controller **302** which includes several state machines to handle the following tasks: packet reception, SM bus interface, and EEPROM updates. Micro-controller **302** sends commands to FIFO control **308** to control data flow from TX FIFO **306**, RX FIFO **310**, and RX Buffer **318**. Micro-controller **302** also responds to SM bus requests from software running on client **104** to access register status **304** or access EEPROM **320**. Signals are received from the MII bus **252** by interface unit **312** and passed to RX FIFO **310**.

Micro-controller **302** accesses EEPROM **320** through EEPROM interface **314** to obtain values to create network packets such as source and destination MAC addresses, IP protocol information, authentication headers, and Universal Data Packet headers. Further, EEPROM **320** retains the Universal Unique Identifier (UUID).

**Figure 3** illustrates a high level flow chart which depicts establishing a unique identifier for each client, and establishing encryption keys for the server and client computer systems in accordance with the method and system of the present invention. The process starts as depicted at block **330** and thereafter passes to block **332** which illustrates establishing a unique identifier for each client which uniquely identifies the particular client computer system. The unique identifier is stored in protected storage **262** in the client which is identified by the unique identifier. Next, block **334** depicts establishing a unique encryption key pair, including a public and private key, for each client. The unique key pair is stored in the client in the protected storage **262**. Thereafter, block **336** illustrates establishing a unique encryption key pair for the server computer system. The unique key pair for the server is stored in the server in protected storage. The process then terminates as illustrated at block **338**.

**Figure 4** depicts a high level flow chart which illustrates a client computer system receiving a primary password and a question and answer combination for an interrogative password method in accordance with the method and system of the present invention. The process starts as depicted at block **400** and thereafter passes to block **402**



which illustrates booting the client computer system. Next, block 404 depicts the client initially receiving a primary password. This primary password will be required during subsequent boot processes in order to gain access to the client. Thereafter, block 406 illustrates the client encrypting the password with the client's private key and server's public key, and transmitting the encrypted password to the server. The process then passes to block 408 which depicts the client receiving a question for an interrogative password method. Block 410, then, depicts the client encrypting the interrogative method question with the client's private and server's public keys, and transmitting the encrypted question to the server along with the client's unique identifier. Thereafter, block 412 illustrates the client receiving a correct answer for the interrogative method which will be associated with the question. Next, block 414 depicts the client encrypting the correct answer with the client's private key and server's public key, and transmitting the encrypted answer to the server along with the client identifier. The process then terminates as illustrated at block 416.

Figure 5 illustrates a high level flow chart which depicts a server computer system storing a primary password and a question and answer combination for an interrogative password method associated with a particular client computer system in accordance with the method and system of the present invention. The process starts as illustrated at block 500 and thereafter passes to block 502 which depicts the server receiving an encrypted primary password from a client computer system, and determining a client identifier which identifies the client which transmitted the encrypted primary password. Next, block 504 illustrates the server

decrypting the primary password utilizing the server's private key and client's public key. Thereafter, block 506 depicts the server storing the decrypted primary password along with the client identifier. The process then passes to block 508 which illustrates the server receiving a message including an encrypted interrogative question.

Block 510, then, depicts the server decrypting the question with the server's private and client's public keys. Thereafter, block 512 illustrates the server storing the decrypted question along with the client identifier. Next, block 514 depicts the server receiving a message including an encrypted correct answer to the question. Thereafter, block 516 depicts the server decrypting the correct answer with the server's private key and client's public key. The process then passes to block 518 which illustrates the server storing the decrypted correct answer to the question with the client identifier and associating the response with the stored question. The process then terminates as illustrated at block 520.

**Figure 6** depicts a high level flow chart which illustrates a server computer system remotely providing a primary password in response to an interrogative password method for a particular client in accordance with the method and system of the present invention. The process starts as depicted at block 600 and thereafter passes to block 602 which illustrates the server receiving a decrypted message from one of the clients 104. The process then passes to block 604 which depicts a determination of whether or not the server was capable of decrypting the message. If a determination is made that the server was not capable of

decrypting the received message, the process passes back to block 602. Referring again to block 604, if a determination is made that the server was capable of decrypting the message, the process passes to block 606 which illustrates the server utilizing the client identifier (ID) which was included within the decrypted message to identify which client sent the message. The process then passes to block 608 which depicts a determination of whether or not the message includes a request for a challenge question. If a determination is made that the message does not include a request for a challenge question, the process passes to block 610 which illustrates processing the message normally.

Referring again to block 608, if a determination is made that the message does include a request for a challenge question, the process passes to block 612 which illustrates the server retrieving a challenge question associated with the client which sent the message. Next, block 614 depicts the server encrypting the challenge question with the server private and client public keys. The encrypted question is then transmitted to the client. The process then passes to block 616 which illustrates the server receiving an encrypted response to the question from the client. Next, block 618 depicts the server decrypting the response using the server private and client public keys. Thereafter, the process passes to block 620 which illustrates a determination of whether or not the response received from the client is the same as the answer stored in the server and associated with this client. If a determination is made that the received response is the same as the stored answer, the process passes to block 622 which depicts the server encrypting and transmitting the primary password stored in

the server and associated with this client to the client. The process then passes back to block 602. Referring again to block 620, if a determination is made that the received response and answer stored and associated with this client are different, the process passes to block 624 which illustrates the server encrypting and transmitting a notice to the client that the received response was incorrect. The process then passes back to block 602.

**Figure 7** illustrates a high level flow chart which depicts a client computer system permitting a user to access the client in response to a receipt of a primary password from a server computer system in response to a successful execution of an interrogative password method in accordance with the method and system of the present invention. The process starts as depicted at block 700 and thereafter passes to block 702 which illustrates the client processing initial POST commands. At this point in the process, the client has begun a booting process but has not yet completed the booting process. Next, block 704 depicts the client prompting a user for a primary password. This is the primary password stored in the client as depicted in **Figure 4**. Thereafter, block 706 illustrates a determination of whether or not a correct password was entered into the client. If a determination is made that the correct password was entered, the process passes to block 708 which depicts the continuation of POST to complete the boot process.

Referring again to block 706, if a determination is made that the correct password was not entered, the process passes to block 710 which illustrates a determination of

whether or not a user has been prompted three times for the entry of the correct password. If a determination is made that the user has not been prompted three times for the entry of the correct password, the process passes back to block 706. Referring again to block 710, if a determination is made that the user has already been prompted three times for the entry of the correct password, the process passes to block 712 which depicts a determination of whether or not the user should be prompted for the interrogative password method. If a determination is made that the user should not be prompted for the interrogative password method, the process terminates as illustrated at block 714.

Referring again to block 712, if a determination is made that the user should be prompted for the interrogative password method, the process passes to block 716 which illustrates the client encrypting a message to the server using the server's public and client's private keys. The message includes the client's identifier and requests the challenge question associated with this client. Next, block 718 depicts the client transmitting the encrypted message to the server. Thereafter, block 720 illustrates the client receiving an encrypted response from the server including the question stored associated with this client. The process then passes to block 722 which depicts the client decrypting the response using the client's private and server's public keys. Block 724, then, illustrates the client displaying the challenge question and prompting for an answer to the question.

The process then passes to block 726 which depicts the client receiving a response to the challenge question, encrypting the response, and transmitting the encrypted

response to the server. Next, block 728 illustrates the client receiving and decrypting a response from the server. Thereafter, block 730 depicts a determination of whether or not the response includes the primary password or a notice. If the response from the server includes a notice, the process passes to block 732 which illustrates the client displaying the notice that the answer provided to the challenge question was incorrect. The process then terminates as depicted at block 734. POST places the system in a condition that requires the user to power off then power on prior to receiving another attempt at entering passwords.

Referring again to block 730, if a determination is made that the response from the server includes the primary password, the process passes to block 736 which depicts the client's network adapter sending the primary password to the BIOS. Thereafter, block 738 illustrates the continuation of the POST commands and the completion of the boot process.

While a preferred embodiment has been particularly shown and described, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the present invention.

**CLAIMS:****What is claimed is:**

1        1.    A method in a data processing system for remotely  
2        recovering a client computer system's primary password, said  
3        primary password being required prior to said client  
4        computer system being accessible by a user, said client  
5        computer system being coupled to a server computer system  
6        utilizing a network, said method comprising the steps of:

7                prior to said client computer system completing a boot  
8        process:

9                        prompting a user to enter said primary password;  
10                        and

11                        providing an interrogative password method in  
12        response to an incorrect entry of said primary  
13        password, said primary password being recoverable from  
14        said server computer system by said client computer  
15        system utilizing said interrogative password method  
16        prior to said client computer system completing said  
17        boot process.

1        2.    The method according to claim 1, further comprising the  
2        step of providing said interrogative password method  
3        including an question and correct answer pair.

1        3.    The method according to claim 2, further comprising the  
2        step of recovering said primary password from said server  
3        computer system in response to a successful completion of  
4        said interrogative method.

1 4. The method according to claim 3, further comprising the  
2 steps of:

3 displaying said question included within said  
4 interrogative method utilizing said client computer system  
5 in response to an incorrect entry of said primary password;  
6 and

7 prompting a user to enter an answer to said question,  
8 wherein an entry of said correct answer will successfully  
9 complete said interrogative method.

1 5. The method according to claim 4, further comprising the  
2 step of:

3 establishing a unique client identifier; and

4 storing said question and said correct answer together  
5 with said unique client identifier in said server computer  
6 system.

1 6. The method according to claim 5, further comprising the  
2 steps of:

3 transmitting a request for said question utilizing said  
4 client computer system in response to an incorrect entry of  
5 said primary password, said request including said unique  
6 client identifier; and

7 transmitting said question utilizing said server  
8 computer system in response to a receipt of said request.



1 7. The method according to claim 6, further comprising the  
2 steps of:

3 transmitting a proposed answer to said question  
4 utilizing said client computer system;

5 determining whether said proposed answer is said  
6 correct answer utilizing said server computer system.

1 8. The method according to claim 7, further comprising the  
2 step of prior to executing said interrogative password  
3 method, permitting a user to initially supply said question  
4 and correct answer pair.

1 9. The method according to claim 8, further comprising the  
2 step of prohibiting access to said client computer system by  
3 prohibiting transmission of said primary password in  
4 response to said proposed answer being unequal to said  
5 correct answer.

1 10. The method according to claim 9, further comprising the  
2 step of completing said boot process in response to said  
3 client computer system receiving said primary password from  
4 said server computer system.

1 11. The method according to claim 10, further comprising  
2 the step of encrypting transmissions between said client  
3 computer system and said server computer system utilizing an  
4 encryption key pair method.

1 12. A data processing system for remotely recovering a  
2 client computer system's primary password, said primary  
3 password being required prior to said client computer system  
4 being accessible by a user, said client computer system  
5 being coupled to a server computer system utilizing a  
6 network, comprising:

7 prior to said client computer system completing a boot  
8 process:

9 means for prompting a user to enter said primary  
10 password; and

11 means for providing an interrogative password  
12 method in response to an incorrect entry of said  
13 primary password, said primary password being  
14 recoverable from said server computer system by said  
15 client computer system utilizing said interrogative  
16 password method prior to said client computer system  
17 completing said boot process.

18 13. The system according to claim 12, further comprising  
19 means for providing said interrogative password method  
20 including an question and correct answer pair.

21 14. The system according to claim 13, further comprising  
22 means for recovering said primary password from said server  
23 computer system in response to a successful completion of  
24 said interrogative method.

1 15. The system according to claim 14, further comprising:

2 means for displaying said question included within said  
3 interrogative method utilizing said client computer system  
4 in response to an incorrect entry of said primary password;  
5 and

6 means for prompting a user to enter an answer to said  
7 question, wherein an entry of said correct answer will  
8 successfully complete said interrogative method.

1 16. The system according to claim 15, further comprising:

2 means for establishing a unique client identifier; and

3 means for storing said question and said correct answer  
4 together with said unique client identifier in said server  
5 computer system.

1 17. The system according to claim 16, further comprising:

2 means for transmitting a request for said question  
3 utilizing said client computer system in response to an  
4 incorrect entry of said primary password, said request  
5 including said unique client identifier; and

6 means for transmitting said question utilizing said  
7 server computer system in response to a receipt of said  
8 request.

1 18. The system according to claim 17, further comprising:

2 means for transmitting a proposed answer to said  
3 question utilizing said client computer system;

4 means for determining whether said proposed answer is  
5 said correct answer utilizing said server computer system.

1 19. The system according to claim 18, further comprising  
2 means for prior to executing said interrogative password  
3 method, permitting a user to initially supply said question  
4 and correct answer pair.

1 20. The system according to claim 19, further comprising  
2 means for prohibiting access to said client computer system  
3 by prohibiting transmission of said primary password in  
4 response to said proposed answer being unequal to said  
5 correct answer.

1 21. The system according to claim 20, further comprising  
2 means for completing said boot process in response to said  
3 client computer system receiving said primary password from  
4 said server computer system.

1 22. The system according to claim 21, further comprising  
2 means for encrypting transmissions between said client  
3 computer system and said server computer system utilizing an  
4 encryption key pair method.

1        23. A data processing system for remotely recovering a  
2        client computer system's primary password, said primary  
3        password being required prior to said client computer system  
4        being accessible by a user, said client computer system  
5        being coupled to a server computer system utilizing a  
6        network, comprising:

7                means prior to said client computer system completing a  
8        boot process, for prompting a user to enter said primary  
9        password;

10               means prior to said client computer system completing a  
11        boot process, for providing an interrogative password method  
12        including an question and correct answer pair in response to  
13        an incorrect entry of said primary password, said primary  
14        password being recoverable from said server computer system  
15        by said client computer system utilizing said interrogative  
16        password method prior to said client computer system  
17        completing said boot process;

18               means for recovering said primary password from said  
19        server computer system in response to a successful  
20        completion of said interrogative method.

21               means for displaying said question included within said  
22        interrogative method utilizing said client computer system  
23        in response to an incorrect entry of said primary password;

24               means for prompting a user to enter an answer to said  
25        question, wherein an entry of said correct answer will  
26        successfully complete said interrogative method;

27               means for establishing a unique client identifier;

28 means for storing said question and said correct answer  
29 together with said unique client identifier in said server  
30 computer system;

31 means for transmitting a request for said question  
32 utilizing said client computer system in response to an  
33 incorrect entry of said primary password, said request  
34 including said unique client identifier;

35 means for transmitting said question utilizing said  
36 server computer system in response to a receipt of said  
37 request;

38 means for transmitting a proposed answer to said  
39 question utilizing said client computer system;

40 means for determining whether said proposed answer is  
41 said correct answer utilizing said server computer system;

42 means for prior to executing said interrogative  
43 password method, permitting a user to initially supply said  
44 question and correct answer pair;

45 means for prohibiting access to said client computer  
46 system by prohibiting transmission of said primary password  
47 in response to said proposed answer being unequal to said  
48 correct answer;

49 means for completing said boot process in response to  
50 said client computer system receiving said primary password  
51 from said server computer system; and

52 means for encrypting transmissions between said client  
53 computer system and said server computer system utilizing an  
54 encryption key pair method.

## ABSTRACT OF THE DISCLOSURE

DATA PROCESSING SYSTEM AND METHOD FOR REMOTE RECOVERY OF A  
PRIMARY PASSWORD

1           A data processing system and method are disclosed for  
2 remotely recovering a client computer system's primary  
3 password. The primary password be correctly entered prior to  
4 the client computer system becoming fully accessible to a  
5 user. The client computer system is coupled to a server  
6 computer system utilizing a network. Prior to the client  
7 computer system completing a boot process, a user is prompted  
8 to enter the primary password. An interrogative password  
9 method is provided in response to an incorrect entry of the  
10 primary password. The primary password is recoverable in  
11 response to a successful execution of the interrogative  
12 password method. The primary password is recoverable from the  
13 server computer system by the client computer system prior to  
14 said client computer system completing said boot process  
15 utilizing the interrogative password method.

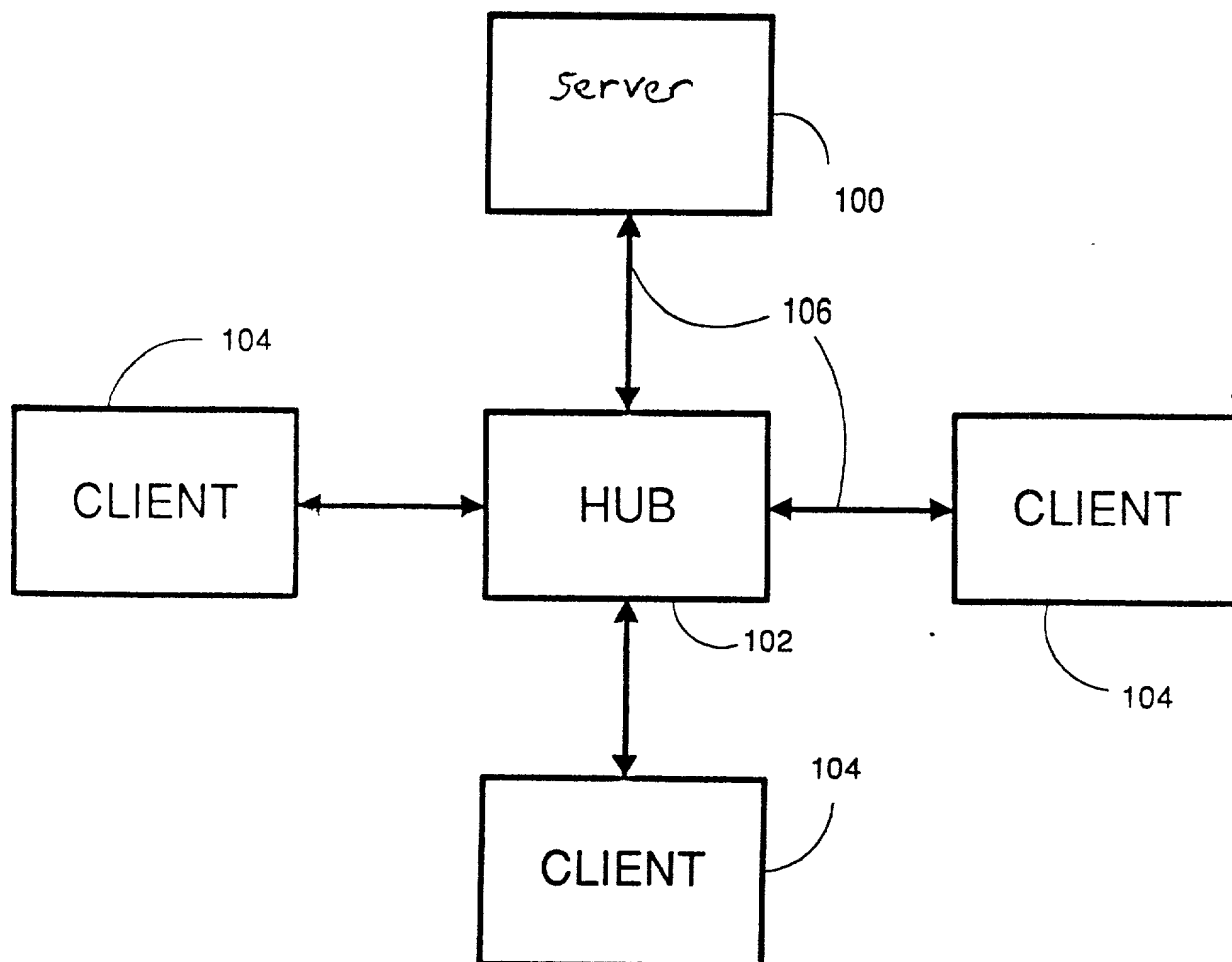
[illegible]

Fig. 1

RP999105



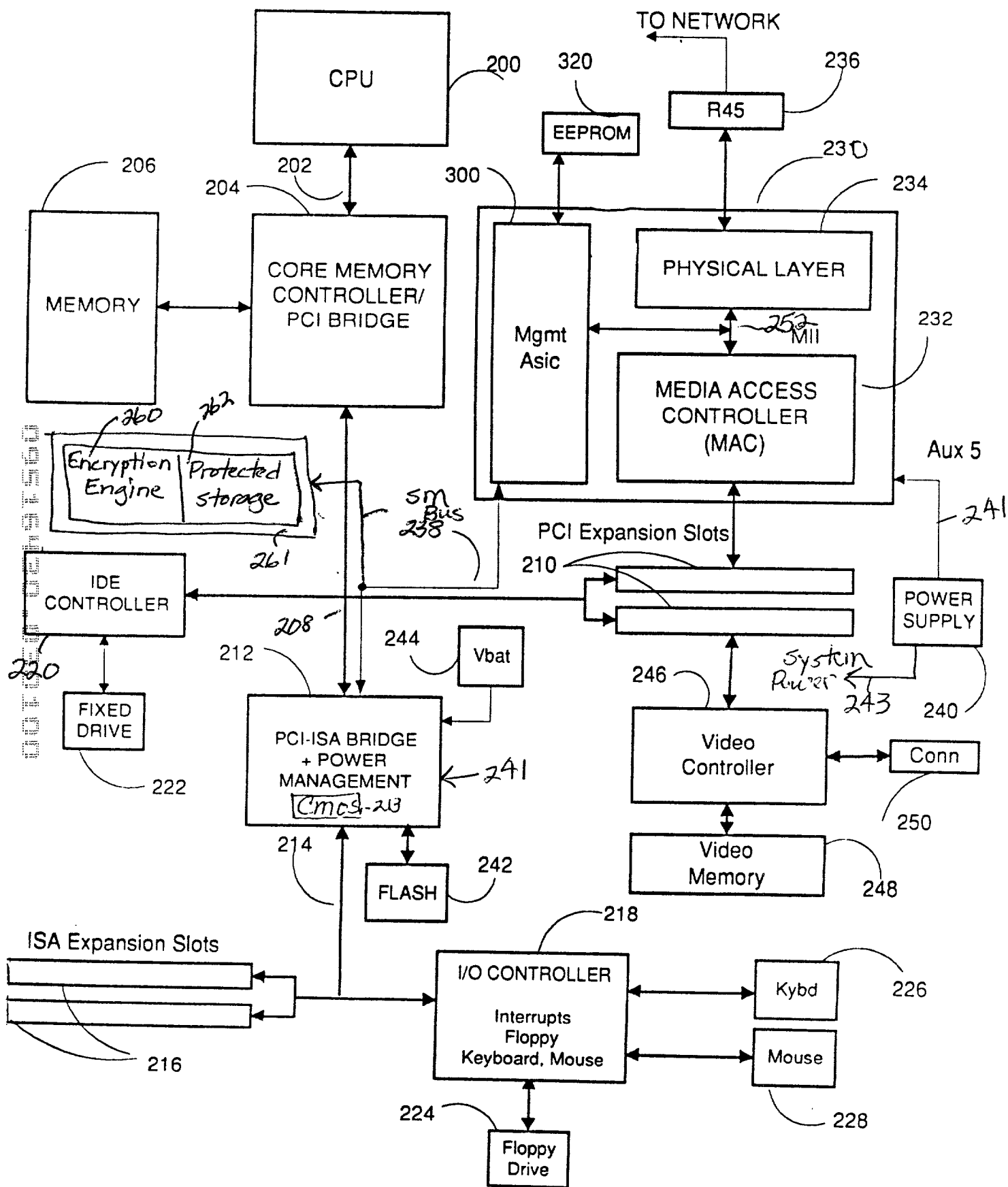


Fig. 2A

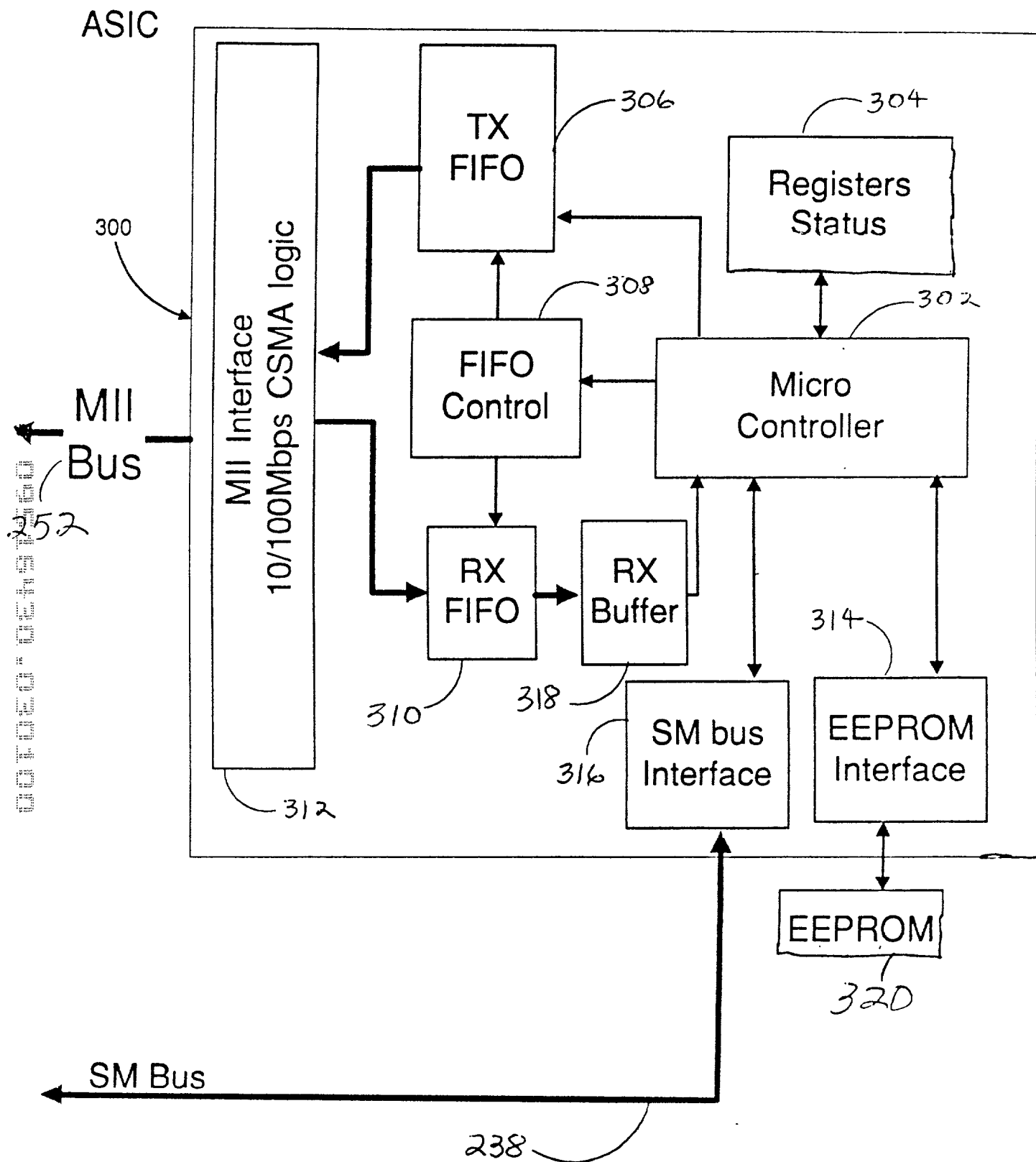


Fig. 2B

RP999105

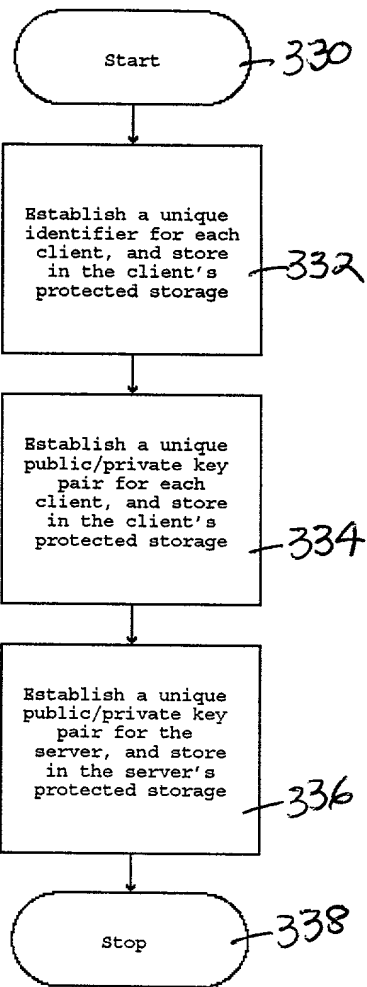


Fig. 3

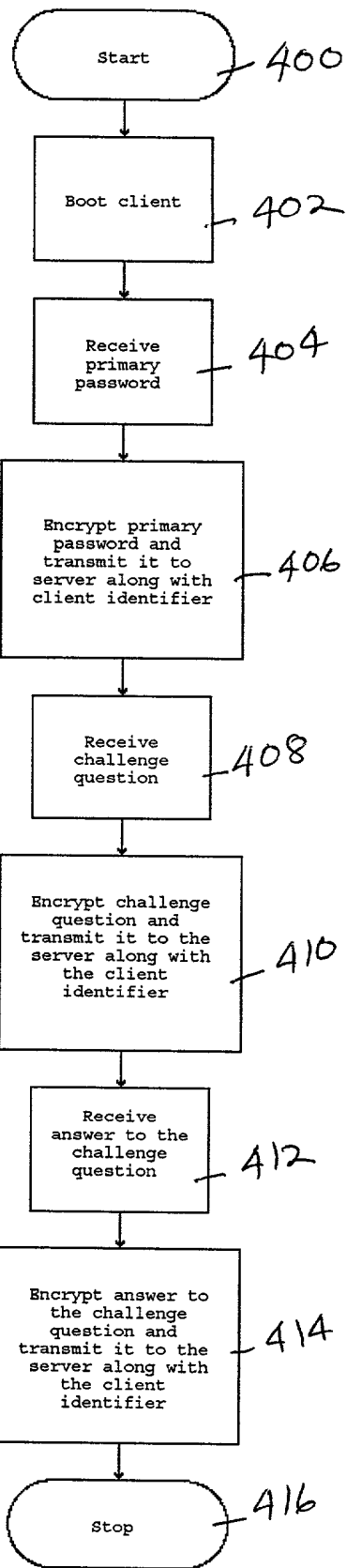


Fig. 4

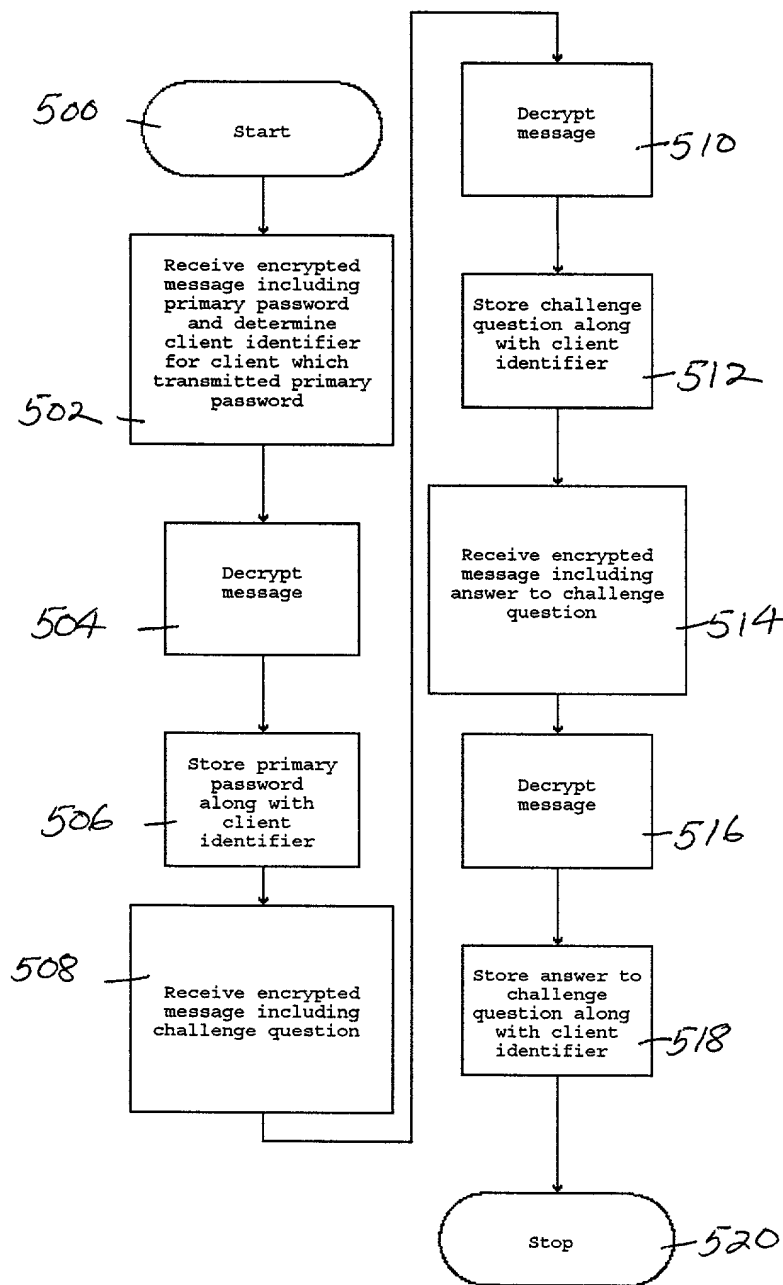


Fig. 5

600 602 604 606 608 610 612 614 616 618 620 622 624

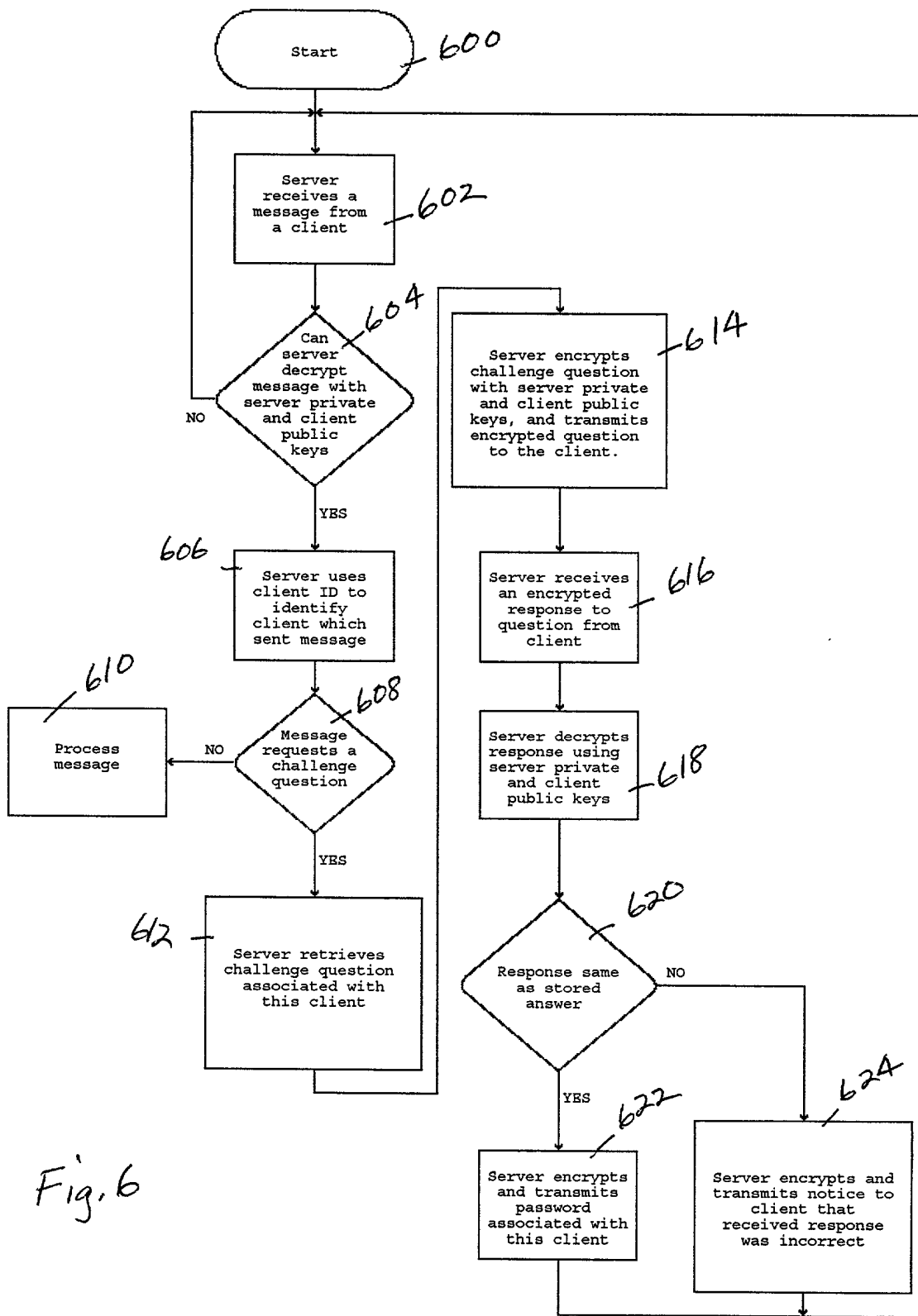


Fig. 6

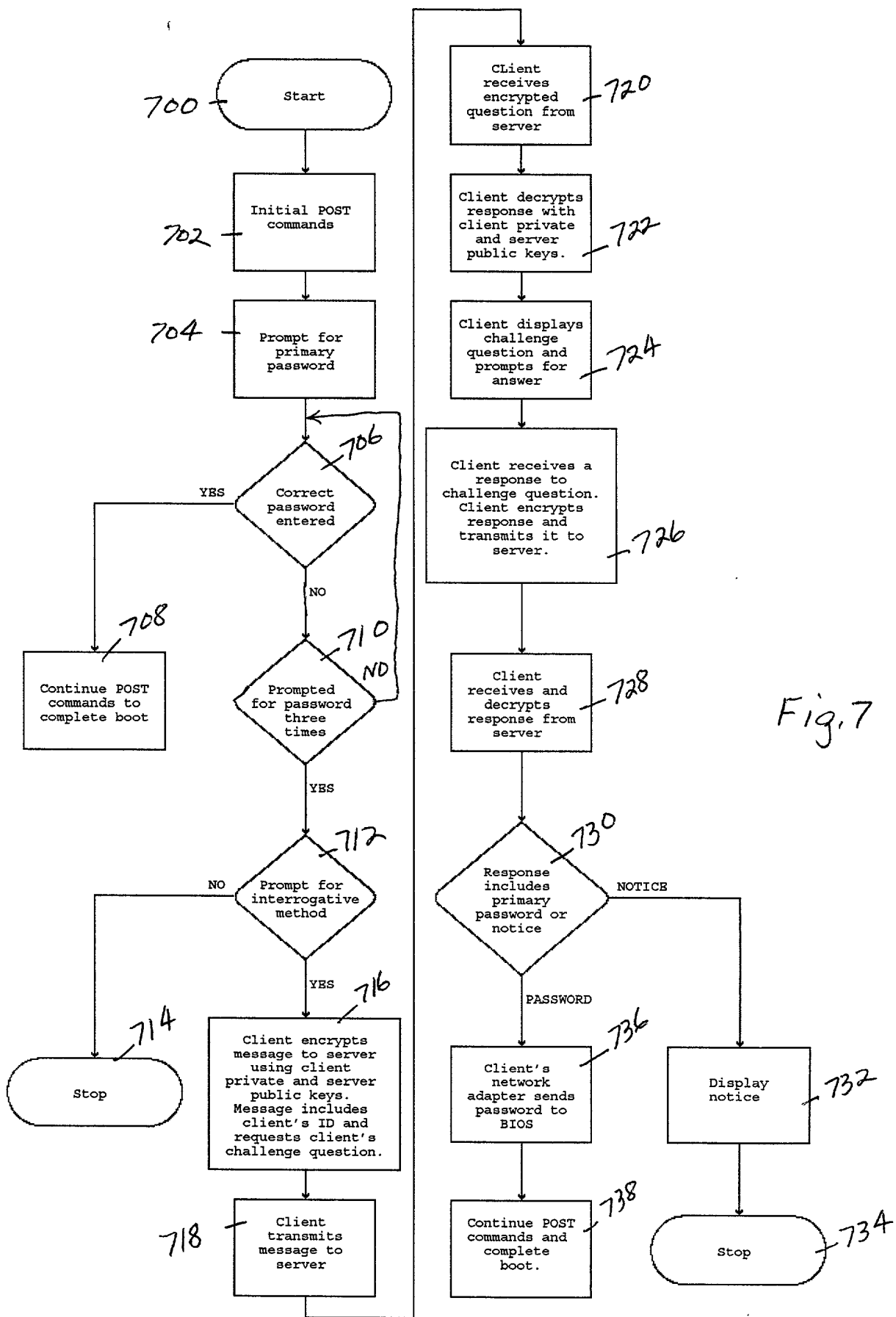


Fig. 7

**DECLARATION AND POWER OF ATTORNEY FOR  
PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

**DATA PROCESSING SYSTEM AND METHOD FOR REMOTE RECOVERY OF A PRIMARY PASSWORD**

the specification of which (check one)

X is attached hereto.

\_\_\_ was filed on \_\_\_\_\_  
as Application Serial No. \_\_\_\_\_  
and was amended on \_\_\_\_\_  
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):			Priority Claimed
_____ (Number)	_____ (Country)	_____ (Day/Month/Year)	___ Yes ___ No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior



application and the national or PCT international filing date of this application:

(Application Serial #)	(Filing Date)	(Status)
------------------------	---------------	----------

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Horace St. Julian, Reg. No. 30,329; Bernard D. Bogdon, Reg. No. 27,773; George E. Grosser, Reg. No. 25,629; Anthony N. Magistrale, Reg. No. 35,595; Daniel E. McConnell, Reg. No. 20,360; Martin J. McKinley, Reg. No. 31,782; Christopher A. Hughes, Reg. No. 26,914; Edward A. Pennington, Reg. No. 32,588; John E. Hoel, Reg. No. 26,279; Joseph C. Redmond, Jr., Reg. No. 18,753; Matthew S. Anderson, Reg. No. 39,093; Matthew W. Baca, Reg. No. 42,277; Michael R. Barré, Reg. No. 44,023; Max Ciccarella, Reg. No. 39,454; Andrew J. Dillon, Reg. No. 29,634; John G. Graham, Reg. No. 19,563; Andrew M. Harris, Reg. No. 42,638; Steven Lin, Reg. No. 35,250; Richard N. McCain, Reg. No. 43,785; Jack V. Musgrove, Reg. No. 31,986; Antony P. Ng, Reg. No. 43,427; Michael E. Noe, Reg. No. 44,975; Brian F. Russell, Reg. No. 40,796; and Daniel E. Venglarik, Reg. No. 39,409.

Send correspondence to: Andrew J. Dillon, FELSMAN, BRADLEY, VADEN, GUNTER & DILLON, LLP, Suite 350, Lakewood on the Park, 7600B North Capital of Texas Highway, Austin, Texas 78731, and direct all telephone calls to Andrew J. Dillon, (512) 343-6116.

FULL NAME OF SOLE OR FIRST INVENTOR: Richard W. Cheston

INVENTOR'S SIGNATURE: *Richard W. Cheston* DATE: 2/25/00

RESIDENCE: 105 Ludgate Court  
Morrisville, North Carolina 27560

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 105 Ludgate Court  
Morrisville, North Carolina 27560

DOCKET NUMBER: RP9-99-105

FULL NAME OF SECOND INVENTOR: Daryl Carvis Cromer

INVENTOR'S SIGNATURE: Daryl Carvis Cromer

DATE: 2/25/2000

RESIDENCE: 206 Haley House Lane  
Apex, North Carolina 27502

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 206 Haley House Lane  
Apex, North Carolina 27502

FULL NAME OF THIRD INVENTOR: Richard Alan Dayan

INVENTOR'S SIGNATURE: Richard Alan Dayan

DATE: 2/25/2000

RESIDENCE: 8308 Wycombe Ridge Way  
Wake Forest, North Carolina 27587

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 8308 Wycombe Ridge Way  
Wake Forest, North Carolina 27587

FULL NAME OF FOURTH INVENTOR: Dhruv Manmohandas Desai

INVENTOR'S SIGNATURE: Dhruv Manmohandas Desai

DATE: 2/25/2000

RESIDENCE: 417 Midenhall Way  
Cary, North Carolina 27513

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 417 Midenhall Way  
Cary, North Carolina 27513

FULL NAME OF FIFTH INVENTOR: Jan M. Janick

INVENTOR'S SIGNATURE: Jan M. Janick

DATE: 2/25/2000

RESIDENCE: 106 Vyne Court  
Morrisville, North Carolina 27560

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 106 Vyne Court  
Morrisville, North Carolina 27560

DOCKET NUMBER: RP9-99-105

FULL NAME OF SIXTH INVENTOR: Howard Jeffery Locker

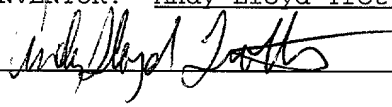
INVENTOR'S SIGNATURE:  DATE: 2/25/00

RESIDENCE: 404 Hogans Valley Way  
Cary, North Carolina 27513

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 404 Hogans Valley Way  
Cary, North Carolina 27513

FULL NAME OF SEVENTH INVENTOR: Andy Lloyd Trotter


INVENTOR'S SIGNATURE:  DATE: 2/25/2000

RESIDENCE: 8203-107 Green Lantern St.  
Raleigh, North Carolina 27613

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 8203-107 Green Lantern St.  
Raleigh, North Carolina

FULL NAME OF EIGHTH INVENTOR: James Peter Ward

INVENTOR'S SIGNATURE:  DATE: 2/25/2000

RESIDENCE: 107 Hemingway Forest Place  
Raleigh, North Carolina 27607

CITIZENSHIP: U.S.A.

POST OFFICE ADDRESS: 107 Hemingway Forest Place  
Raleigh, North Carolina 27607